PRA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,851	05/22/2001	Ralph S. Hoefelmeyer	COS 00 017	8371

25537 7590 05/19/2004

MCI, INC
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW, 10TH FLOOR
WASHINGTON, DC 20036

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 05/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/862,851	Applicant(s) HOEFELMEYER ET AL.	
	Examiner Taghi T. Arani	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *2/24/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-30 were pending for examination.

Claims 31-32 are newly added.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 4 recites the limitation "the detection manager" in line 1. There is insufficient antecedent basis for this limitation in the claim.

For purpose of applying art, the examiner assumes "the remote site detection system"

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6-7, 9, 14-15, 17-20, 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, JI et al, US Pat. No. 5,623,600, issued April 1997 and further in view of Shanklin et al., US Pat. No. 6,578,147, filed Jan. 1999.

As per (Amended) claims 1, 9, JI is directed to a method and system for detecting and elimination viruses on a computer network which includes a File Transfer Protocol (FTP) proxy server, for controlling transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system, see abstract.

In a preferred embodiment, Ji discloses a gateway node (corresponding to a front-end processor) comprising a File Transfer protocol proxy server and a Simple Mail Transfer protocol proxy server for detecting (scanning) viruses (i.e. malicious code) in file transfers and messages and controlling data transfers to and from the gateway to and from a given network of which the gateway node is part, see col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40.

JI teaches that if a virus is detected, the proxy servers respond in variety of ways (i.e. countermeasures taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory on the proxy server and notify the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of JI clearly suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined to have a malicious code (i.e. virus) and the user is notified (i.e. an alarm is generated)

Ji fails to teach "a plurality of scanning computer systems" and distributing " copies of the flow to each of the scanning computer systems in parallel for scanning"

However, Shanklin is directed to a method of detecting unauthorized access on a network indicated by signature analysis of packet traffic on the network. A plurality of detection sensors (i.e. scanners) are connected at a network entry point associated with an internetworking device (i.e. a front- end) , see col. 1, line 61 through col. 2, line 19. Signatures detected by Shanklin's sensors include those associated with malicious intent attack (i.e. malicious codes), denial of service attack, and other method of misuse.

Shanklin teaches that the internetworking device (i.e. a front end processor) inspects packets incoming from the external network and a load balancing unit implemented in the internetworking device performs a "copy to "operation to send each packet to the sensors (i.e. a copy of the flow), see col. 6, lines 25-46, where in a detection engine examines and analyses each packet and if the analysis indicates a misuse (or a malicious code), the sensor sends an alarm to a separate detection management station (i.e. a detection management system) to take action (i.e. countermeasure), see col. 3, lines 55-65, see also col.4, line 54 through col. 5, line 7.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ji's Gateway to include parallel sensors of Shanklin to provide a virus detection system that can keep up with the high traffic throughput of today's network, see Shanklin's col. 2, lines 14-19, specially when Ji is also concerned in effectively detecting and eliminating viruses without significantly affecting the performance of the computer, see JI col. 2, lines 30-36.

As per claims 6 and 14, JI teaches that the apparatus of his invention, in particular the FTP proxy server and the SMTP proxy server could be includes on a FTP server or a world wide server for scanning files and messages as they are downloaded from the web, see col. 5, lines 28-

38. This clearly suggests that Ji's invention includes the flow of Hypertext markup file and a transferred file.

As per claims 7 and 15, JI teaches that if a virus is detected, the proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of JI clearly suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined.

Claims 17- 19 are apparatus, method and a computer –readable medium claims corresponding to claims 1 and 6. Claims 17-19 are rejected as such.

Claim 20 is an apparatus claim reciting limitations of claims 1 and 6. Claim 20 is rejected for the same reasons provided in the statement of rejections of claims 1 and 6 above.

(Amended) claims 22-23 are apparatuses implementing features of claims 1, 6 and 7. Claim 22 is rejected as such.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-4, 10-12, 24-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji et al. and Shanklin et al as applied to claims 1and 9 above, and further in view of Wells, US. Pat. No. 6,338,141, filed Sept. 1998.

As per claims 2- 4, 10-12, JI-Shanklin fail to teach a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer system" , and updating the detection system by the detection manager.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses , are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Shanklin to provide a virus detection system with high degree of certainty

and to avoid false identification while recognizing new variants of known viruses, see col.2, lines 22-46.

(Amended) claim 24 is an apparatus reciting limitations of claims 1, 2 and 4. Claim 24 is rejected as such.

(Amended) claims 25, 27 and claim 26 recite limitations (broader in scope) of apparatus claims 1, 2, 4, 6 and 7. Claims 25-27 are rejected for the same reasons provided in the statement of rejections of claims 1,2,4,6 and 7 above.

Claims 28-30 are computer-readable medium implementing steps of claims 1- 4, 6 and 7. Claims 28-29 are rejected for the same reasons provided in the statement of rejections of claims 1-4 and 6-7.

Claims 5, 13, 21 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji and Shanklin as applied to claim 1 above, and further in view of Xu , US Patent Application Publication 2002/0032766, published Mar. 2002.

As per (Amended) claim 5, claims 13 and 31-32, Modified Ji- Shanklin fails to teach scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code.

However, the Examiner asserts that the use of multiple virus scanning devices with different detection software and with different coverage of malicious code is well known in the art.

It would have been obvious to one of ordinary skill in the art to modify the modified Ji-Shanklin's parallel sensors to incorporate virus scanning software differ in their capabilities be

used as a "safety net" to improve the chances of detecting a virus, see page 18, paragraphs 228 (Xu).

Claim 21 is method claim reciting limitations (broader in scope) of claims 1,5 and 6. Claim 21 is rejected for the same reasons provided in the statement of rejections of claims 1, 5 and 6 above.

Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, JI et al,(US Pat. No. 5,623,600), Shanklin et al.(US Pat. No. 6,578,147), Wells(US. Pat. No. 6,338,141) and further in view of Xu , US Patent Application Publication 2002/0032766.

(Amended) claim 8 is an apparatus reciting limitations of claims 1-7.

That is, modified JI- Shanklin-Wells teaches "A system for malicious code detection, comprising:

a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat (see the statement of rejections of **claims 2-3** above);

Modified modified JI- Shanklin-Xu teaches"a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for scanning content for malicious code and generating an alarm when the content contains malicious code (see the statement of rejection of claims **1** and **5** above); and

Modified JI- Shanklin teaches a front-end processor, coupled to the scanning

computer systems, configured for receiving a flow of content from an external network and distribution a copy of the flow to each of the scanning computer systems in parallel for scanning, said flow including at least one of a hypertext markup file and a transferred file (see the statement of rejections of claims **1 and 6** above); and

a detection management system, coupled to the scanning computer systems, configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computer systems generates an alarm on the piece of malicious code (see the statement of rejections of **claims 1 and 2** above);

employing a countermeasure on the flow if at least one of the scanning computer systems generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems (see the statement of rejections of claims **1 , 4 and 7** above).

Claim 8 is rejected for the same reasons provided in the statement of rejections of claims 1-7 above.

(Amended) claim 16 is a method claim reciting limitations (broader in scope) of apparatus claim 8 . Claim 16 is rejected for the same reasons provided in the statement of the rejections of claims 8 and 1-7 above.

Response to Amendment

Applicant's arguments filed on 2/24/2004 regarding the rejection of the claims 1-30 under 35 U.S.C. 103() have been fully considered but in view of the new ground of rejection provided above they are not persuasive. Applicant's attempt to distinguish the claims from prior art is based on noting the lack of a teaching of a "distributing a copy of the flow to each of scanning computer systems in parallel ", "duplicating the flow to produce a plurality of copies of the flow" recited in independent claims 1,8,9, 16,17, 18 and 19 and "receiving respective copies of a flow of content from the front-end processor in parallel" recited in claim 20-21 and "receiving an alarm when a flow of content scanned by the scanning computer system in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred file', see page 13, last paragraph.

This features was found to be taught by modified Ji- Shanklin-Wells-Xu as discussed in the rejections of claims 1-32 above.

As per Applicant's arguments relating to rejection of claims 1 and 9 and *Shanklin et al.* reference, the Applicant argues that *Shanklin et al.* sends different packets to each of multiple processors and that each sensor *Shanklin et al.*, receives a portion of traffic, page 14. Applicant further argues that each sensor of *Shanklin et al.*, is identical to the other sensors .

The Examiner responds that different sensors (in contrast with identical sensors of *Shanklin et al.*,) are not claimed at least in claims 1 and 9 and receiving a "portion of traffic" by *Shanklin's* sensors is clearly encompasses receiving "a copy of the flow" recited in claims 1 and 9.

As per Applicant argument relating to the rejection of claims 2-4,10-12,16-30 and *Wells* reference, the Applicant argues that *Wells* does not mention " distributing anything to scanning computer systems "in parallel", page 16, second paragraph.

The Examiner Acknowleges that Wells is a secondary reference in a 103 () type rejection and that *Wells* is adirected to a collection of relational data comprising various relational signature objects created from viruses. That is, Wells reference is used to fill in the gap for the limitation "a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer system" , and updating the detection system by the detection manager recited in claims 2-4, 10-12.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100